[This question paper contains 4 printed pages.]

Your Roll No.............

Sr. No. of Question Paper : **1298** **A**

Unique Paper Code : 32357610

Name of the Paper : DSE-4 (Number Theory)

Name of the Course : **CBCS (LOCF) – B.Sc. (H) (Mathematics)**

Semester : VI

Duration : 3 Hours Maximum Marks : 75

Instructions for Candidates

1. Write your Roll No. on the top immediately on receipt of this question paper.
2. **All** questions are compulsory.
3. Attempt any **two** parts of each question.
4. Question Nos. **1** to **3**, each part carries **6.5** marks and Question Nos. **4** to **6**, each part carries **6** marks.

1. (a) Determine all solutions in the integers of the Diophantine equation $24x + 138y = 18$.

   (b) A farmer purchased 100 head of livestock for a total cost of Rs. 4000. Prices were as follow: calves, Rs. 120 each; lambs, Rs. 50 each; piglets,

P.T.O.

Rs. 25 each. If the farmer obtained at least one animal of each type, how many of each did he buy?

(c) Write a short note on Goldbach conjecture.

(d) Find the remainder obtained upon dividing the sum $1! + 2! + 3! + \cdots + 100!$ by 12.

2. (a) Prove that the congruences

$x \equiv a(\text{mod } n)$ and $x \equiv b(\text{mod } m)$ admits a simultaneous solution if $\gcd(n,m)|(a-b)$; if a solution exists, confirm that it is unique modulo $1\text{cm}(n,m)$.

(b) Solve the linear congruence $25x \equiv 15 \pmod{29}$.

(c) If p an q are distinct primes, prove that

$$p^{q-1} + q^{p-1} \equiv 1(\text{mod } pq).$$

(d) State and prove Wilson's theorem.

3. (a) If f is a multiplicative function and F is defined by $F(n) = \sum_{d/n} f(d)$ then show that F is also multiplicative, explain your result when m = 8 and n = 3.

(b) Explain Mobius μ- function with example and also show that

$$\mu(n)\mu(n+1)\mu(n+2)\mu(n+3) = 0$$

for each positive integer n.

(c) Use the fact that each prime p has a primitive root to give a different proof of Wilson's theorem.

(d) Let r be a primitive root of the integer n. Prove that r^k is a primitive root of n if and only if $\gcd(k, \Phi(n)) = 1$.

4. (a) Define number – theoretic function and also show that number – theoretic functions σ and τ both are multiplicative functions.

(b) Write a short note on Mobius function and show this function is multiplicative function.

(c) If p is a prime and $k > 0$, then prove $\phi(p^k) = p^k - p^{k-1}$. Explain your result by an example.

(d) Use Euler's theorem for any odd integer a, to prove $a^{33} \equiv a(\text{mod } 4080)$.

5. (a) Find a primitive root for any integer of the form 17^k.

(b) Let p be an odd prime and gcd(a, p) = 1. Then prove that 'a' is a quadratic residue of p if and only if $a^{(p-1)/2} \equiv 1 \pmod{p}$.

(c) Let p be an odd prime and let a and b be integers that are relatively prime to p. Show that (ab/p) = (a/p) (b/p).

(d) Find the value of Legendre symbols (18/43) and (–72/131).

6. (a) Use Gauss lemma to compute Legendre symbol (5/19).

(b) Show that 7 and 18 are the only incongruent solutions of $x^2 \equiv -1 \pmod{5^2}$.

(c) Using the linear cipher $C \equiv 5P + 11 \pmod{26}$ encrypt the message CRYPTOGRAPHY.

(d) Use the Hill's cipher

$$C_1 \equiv 5P_1 + 2P_2 \pmod{26}$$

$$C_2 \equiv 3P_1 + 4P_2 \pmod{26}$$

to encrypt the message GIVE THEM TIME.